Crypto.Sec Group

http://crypto.di.uoa.gr

Aggelos Kiayias

Crypto.Sec Group

Crypto.Sec Group

- New group in department (formed in 2009).

Crypto.Sec Group

- New group in department (formed in 2009).
- 1 supervisor, 2 Grad students, 3 undergrads engaged in research projects.

Crypto.Sec Group

- New group in department (formed in 2009).
- 1 supervisor, 2 Grad students, 3 undergrads engaged in research projects.
- Currently expanding :
  hiring 3 new Ph.D. + 1 Post-Doc.

Group Activities

- Research : Cryptography & Computer Security.
- Teaching : Cryptography (7th Semester), Computer Security (8th Semester).
- Outreach & Collaborations : participated in national and NATO Cybersecurity exercises. Ongoing collaborations with Google Research and AT&T Research.
- Organization : organized CT-RSA : the Cryptographers' Track at RSA conference 2011.

Current Funding

- European Research Council - Starting grant. 1,200,000 Eur

- Marie Curie Program 100,000 Eur

Research Foci

Cryptography

- How to express security in mathematical terms ?
- How to design systems that are immune to attacks ?
- How to formally argue that a system is secure ?
- How to analyze systems for vulnerabilities ?

Computer Security

current crypto.sec research

sampling of some of our ongoing work

current crypto.sec research

sampling of some of our ongoing work

1. Definitional aspects of security. How to define security? What are the fundamental differences between secure tasks ?

If a box implements f can we use it to perform g ?

current crypto.sec research

sampling of some of our ongoing work

1. Definitional aspects of security. How to define security? What are the fundamental differences between secure tasks ?

If a box implements f can we use it to perform g ?

2. Controlling data movement. How to throttle, manage and trace information online as it flows from content producers to content consumers?

if a movie is distributed in a controlled fashion to a set and subsequently exposed, who is the source of the leak?

current crypto.sec research

sampling of some of our ongoing work

current crypto.sec research

sampling of some of our ongoing work

3. Identity Management with Privacy. How to maintain anonymity of identities while performing security critical tasks?

How to achieve minimum disclosure of personal data while gaining access to entitled resources?

current crypto.sec research

sampling of some of our ongoing work

3. Identity Management with Privacy. How to maintain anonymity of identities while performing security critical tasks?

How to achieve minimum disclosure of personal data while gaining access to entitled resources?

4. Privacy in databases. How to access data while minimizing exposure of access patterns ?

How to achieve minimum disclosure of data according to the intended functionality?

current crypto.sec research

sampling of some of our ongoing work

current crypto.sec research

sampling of some of our ongoing work

5. Web Application Attacks. How secure are web-applications? Browser is a multi-layer operating environment - can it be exploited?

We are developing and seek ways to protect against Side-channel attacks against the web-application state

current crypto.sec research

sampling of some of our ongoing work

5. Web Application Attacks. How secure are web-applications? Browser is a multi-layer operating environment - can it be exploited?

We are developing and seek ways to protect against Side-channel attacks against the web-application state

6. Proofs of Secure Erasure. How to prove you forgot something?

How to be convinced there is no malicious code lurking in your system's memory?

current crypto.sec research

sampling of some of our ongoing work

current crypto.sec research

sampling of some of our ongoing work

7. Security in social networks. Can we utilize and benefit from social network structures while maintaining privacy from system servers?

We are developing new methods of encrypting social network related data and finding more secure ways of sharing.

current crypto.sec research

sampling of some of our ongoing work

7. Security in social networks. Can we utilize and benefit from social network structures while maintaining privacy from system servers?

We are developing new methods of encrypting social network related data and finding more secure ways of sharing.

8. Traffic analysis for malicious activity.

Searching needles in hay stacks.

How to parse data from large network traffic junction points and detect malicious communication patterns?

Cryptography Class

- A research oriented cryptography course.
  - Provable security approach with firm grounds on Computational Complexity.
    Probabilistic algorithms.
    Number theory.

Coin flipping protocols, key exchange protocols, digital signatures, zero-knowledge protocols and identification, public-key encryption, blind signatures, homomorphic encryption, secret-sharing, secure function evaluation, universal composability.

Computer Security Class

- Comprehensive approach to security. Hands-on projects and experimentation.
  - Project #1 : Buffer Overflow Laboratory. Cracking into superuser accounts in linux systems.
  - Project #2 : Web-authentication. Recognizing who you talk to over http.
  - Project #3 : Man-in-the middle Laboratory. Descrambling secure networking protocols.
  - Project #4 : Web Wars. Defense & Offense. **Capture the flag**.

Questions / Discussion