Report on DIMACS* Tutorial on Applied Cryptography and Network Security

Date of tutorial: August 4 – 7, 2003

Tutorial Organizer:

Rebecca Wright, Stevens Institute of Technology

Primary Lecturer:
Amir Herzberg, Bar-Ilan University

Additional Lecturers:
Markus Jakobsson, RSA Laboratories
Angelos Keromytis, Columbia University
Hugo Krawczyk, Technion and IBM Research
Rebecca Wright, Stevens Institute of Technology

Problem Session Leader:
Nelly Fazio, New York University

Report Author:
Geetha Jagannathan, Department of Computer Science
SUNY at Stony Brook

Date of report: December 3, 2003

*DIMACS was founded as a National Science Foundation Science and Technology Center. It is a joint project of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, with affiliated partners Avaya Labs, IBM Research, Microsoft Research, and HP Labs.

1 Tutorial Focus

The intention of this tutorial was two-fold. One, it was a stand-alone condensed course on cryptography and its applications to secure networking and electronic commerce, giving an introduction to some of the fundamental issues in this field. Two, it was designed to provide background knowledge to researchers and graduate students who wished to participate in the DIMACS Special Focus on Communication Security and Information Privacy. The tutorial appears to have been successful in both regards. For example, several graduate student participants have returned or plan to return for later workshops in the special focus and have said that they feel the tutorial helped them to get more out of the workshops than they otherwise would have. Another participant, a professor at an undergraduate college, was attending the tutorials in order to help him with curriculum development in cryptography and security at his college. On a more personal level, due to interactions initiated at the tutorial, the author of this report is now a Ph.D. student at Stevens Institute of Technology under the guidance of workshop organizer Dr. Wright.

Each tutorial day included both lectures and problem sessions. The following were the topics of the lectures:

- cryptographic primitives and protocols: symmetric key cryptography, public key cryptography, authentication, and key exchange protocols
- key management and access control: public key infrastructures and trust management
- network security: snooping, spoofing, distributed denial of service attacks, SSL, SSH, IPsec.
- electronic commerce: electronic payments protocols, auctions

There were 41 participants in the tutorial in addition to the 5 lecturers. The academic participants included slightly more students than faculty. About a quarter of the participants were from industry. In addition to the United States participants, there were students and faculty from South Korea and Canada.

2 Summary of Presentations

2.1 Principles of security, modern cryptography and symmetric encryption

Speaker: Amir Herzberg

In this talk Dr. Herzberg introduced to the audience the basic principles of security and modern cryptography. He began by discussing from the layman's point of view the general concept of security and ways to prevent damage in spite of adversarial attacks. His talk then moved to a more formal information-theoretic perspective of the same concepts of security.

Dr. Herzberg introduced and distinguished between the different concepts of symmetric key and public key cryptography. Both modes of cryptography are based on Kerckhoff's design principle, which states that the adversary knows the whole design except the secret keys. This talk focused on symmetric key (or shared key) cryptography. The goal here is to transform the secret message (plaintext) into garbled ciphertext such that any adversary can gain no information about the plaintext from the ciphertext in a reasonable amount of computation time. He gave some examples of early simple ciphers used by Julius Caesar and others, and showed that some of them are easily broken. He then explained Shannon's notion of an unconditionally secure encryption scheme. Shannon's theorem states that a necessary condition for perfect security is that the length of the key should be at least as large as the length of the message. The next part of the talk was about early stream ciphers such as polyalphabetic ciphers and Vigenere's cipher. He showed how these examples could be broken under various attacks.

Dr. Herzberg then discussed the conditions necessary to construct a good block cipher. In this context he spoke about pseudo-random functions and pseudo-random permutations, and about ways of constructing one from the other. He also discussed practical block ciphers such as DES, triple DES and AES.

He spoke about the infeasibility of perfect security in practice and discussed the minimum assumptions made to achieve security in practice. He also addressed issues such as the usefulness of block ciphers in practice and various modes of using them. Finally, Dr. Herzberg discussed the ways of constructing cryptosystems that are secure against polynomially indistinguishable chosen plaintext and chosen ciphertext attack. He concluded his talk by reiterating a fundamental principle of cryptography: "Security re-

quirements should be sufficient, simple and should allow practical (efficient) solutions."

2.2 Advanced Encryption Standard(AES): Rijndael

Speaker: Arta Doci (tutorial participant)

Ms. Doci's talk was about the Advanced Encryption Standard. Created by Vincent Rijmen and Joan Daemen, this is a symmetric key block cipher. She explained that speed and cost are the two factors that make symmetric encryption suitable for encrypting large amounts of data. She laid out the characteristics of the Rijndael algorithm as a byte-oriented iterated block cipher scheme, and explained the two key objectives of any good block cipher as given by Shannon, namely:

- Confusion—which can be achieved through substitution operations, and
- Diffusion—which can be achieved through permutation operations

Shannon's generic algorithm breaks each block of plaintext data into smaller pieces. Each piece is then passed in parallel through an S-box (Substitution box) and a P-box (Permutation box). In the Rijndael algorithm, the plaintext is broken into 128-bit blocks (16-byte blocks), and each block is viewed as a 4×4 matrix. The algorithm proceeds in rounds. In each round the bytes in the matrix go through the steps of

1. Substitution, where each byte of the matrix is substituted using an S-box,
2. row shifting, where row i is left-rotated by i steps,
3. column mixing, which multiplies each column by a mixing polynomial, and
4. finally the key for that round is XORed with the matrix.

After the requisite number of rounds is complete, the resulting matrix is output.

Ms. Doci explained that the Rijndael algorithm operates in the finite field GF(256). She then focused on the mathematics behind the algorithm. She defined various concepts such as finite fields, their characterization, cyclic groups, etc. She explained to the audience various number theoretic

algorithms, especially those on finite fields. In particular, she showed how to compute the multiplicative inverse of an element in GF(256). The substitution step of the Rijndael algorithm is essentially the substitution of each byte in the 4×4 matrix by its multiplicative inverse.

Ms. Doci concluded the talk by emphasizing that the strength of the Rijndael algorithm arises from its security against known attacks, its elegant mathematical structure, and its efficiency.

2.3 Hashing

Speaker: Amir Herzberg

In this talk Dr. Herzberg spoke about cryptographic hash functions. He started by delineating the properties desired of any such function $h(x)$, namely:

- compression—the transformation of long (and potentially unbounded) input to a small output
- confidentiality—the infeasibility of computing x given $h(x)$ (that is, the inverse function should not be easy to compute)
- collision resistance—the strong form of this property demands that it be infeasible to find x and x' such that $h(x) = h(x')$; the weak form requires that given x, it should be infeasible to find an x' such that $h(x) = h(x')$.
- randomness—the output should be uniformly distributed.

He then spoke about the random oracle methodology for analyzing cryptographic systems. The assumption here is that $h(x)$ is a random function, which is not quite accurate since $h(x)$ is fixed. However, this method does help in quickly screening out insecure solutions.

Although hash functions satisfy the confidentiality property, they have no secret key, and hence they cannot be used to send secret messages. However, hash functions are one way and hence do not allow anyone to deduce the input from the output. In general a one way function $f(x)$ is one which

- Can be computed by a probabilistic polynomial time algorithm, and
- No other probabilistic polynomial time algorithm, which is given any $f(x)$, can compute a y such that $f(y) = f(x)$. (More precisely, the probability that such a y can be computed is almost zero.)

This definition is only asymptotic, and a hash function that satisfies the above properties may actually reveal partial information about the input.

Dr Herzberg then explained strong and weak (second pre-image) collision-resistant hash functions. He said that the former, though natural, is hard. An adversary may just output a specific, precomputed collision in the hash function. In the latter, we simply claim that it is hard to find a collision for a specific (randomly chosen) input x. He discussed one potential use of hash functions as a signature method. This requires the use of randomness.

The next topic in the talk was about designing collision-resistant hash functions. Since it is hard to build variable input length hash functions directly, one idea is to build them on top of fixed input length hash functions. He explained the Merkle-Damgard technique for this process. He quoted examples of standard hash functions such as MD5, SHA-1 and RIPEMD.

2.4 Message Authentication Codes: MAC

Speaker: Hugo Krawczyk

Dr. Krawczyk started the talk by motivating the audience on the need for authentication. He differentiated between the concepts of entity authentication and data authentication. In the data authentication scheme the sender appends to the data a signature or finger print that the receiver can verify and no one else can forge. It is called a digital signature in the public key model and message authentication code (MAC) in shared key cryptosystems.

Dr. Krawczyk explained several common scenarios in which MACs are used. They include SSL, SSH, IPsec, etc. He spoke about security issues in MAC, and about various MAC attacks on CBC encryption. He also showed that CBC is insecure if messages are of variable length. After presenting various MAC constructions including CBC-MAC, HMAC and UMAC, he explained the security in each of them. The CBC-MAC is based on block ciphers. HMACs are based on cryptographic hash functions. Finally he spoke about ϵ-almost XOR universal (AXU) hashing and showed how to build AXU families. These are pure combinatorial objects with no cryptographic assumptions. He concluded the talk by giving references to some AXU constructions.

2.5 Public Key Cryptography

Speaker: Rebecca Wright

Dr. Wright's talk was about public key cryptography. She started the talk with a brief overview of public key encryption, Diffie-Hellman key exchange and digital signatures. She discussed the advantages and disadvantages of symmetric encryption. Although symmetric encryption provides very efficient solutions, n users of such a system would need $O(n^2)$ keys, and all keys need to be agreed on securely. But in public key cryptography, the key used for encryption is made public and the decryption key is kept private.

Dr. Wright presented the necessary number theoretic results that underlie public key cryptography. She defined trapdoor one-way functions and showed how it is used in RSA. In fact, there are no strictly proven trapdoor one-way functions. She also talked about how to choose the parameters in RSA to prevent the adversary from breaking the cryptosystem. The security of RSA assumes that factorization is believed to be computationally hard. The best-known factorization algorithms such as quadratic sieve have super-polynomial time complexity. She then covered various adversarial models.

Dr. Wright next spoke about Diffie-Hellman key exchange and digital signatures. She then focused on the various kinds of forgeries on signatures and showed how hash functions help to solve this problem. Finally, she gave a few examples of signature schemes such as the El Gamal Signature Scheme. She concluded the talk by briefly indicating the recent advances in public key cryptography.

2.6 Public Key Infrastructures, Access Control and Trust Management

Speaker: Amir Herzberg

In this talk, Dr. Herzberg focused on public key certificates, identity in certificates, certificate authorities, certificate validation and certificate revocation. He spoke about the usefulness of public keys in encrypting data and in signing documents. He then addressed the issue of how to obtain the public key. The certification authority signs the certificate binding the public key to a person's identity. He spoke about the public key certificate and various attributes involved and the distinguished name hierarchy.

In the second half of the talk, Dr Herzberg focused on the validation

of the certificate path. He indicated a few measures like local validation of each certificate and verifying each certificate. In this context, he spoke about the certificate path discovery problem. The offline version of the problem is stated as follows: given a set of (locally valid) public key certificates, is there a certificate path to Alice's certificate? This problem can be viewed in terms of a graph and the solution is to determine the shortest path.

Later Dr. Herzberg discussed the risks involved in identity public key certificates such as exposure of CA private signing key and issuing certificates for false identity. Finally Dr. Herzberg explained various reasons for revoking certificates such as key compromise, CA compromise and change in affiliation. He concluded his talk emphasizing the fact that public key certificates form a link between public key and its owner.

2.7 Resilience to Key Exposure: Revocation, Forward Security, Secret sharing, Threshold and Proactive Security

Speaker: Amir Herzberg

Dr. Herzberg began his talk by speaking about the weak security we have in current operating systems, and how data corruption and key exposures are possible. He then addressed the issue of obtaining secure services from insecure servers and about protecting data on insecure servers. In this context, he mentioned the password scheme where the user password is encrypted during a session. The adversary can launch a dictionary attack, which can be prevented using salting techniques.

Dr. Herzberg then spoke about the various problems regarding the exposure of secret keys, and the measures to be taken to safeguard against them. He later discussed more advanced issues such as how to protect past traffic, and what happens to old signatures. The solutions to these problems include (i) time stamping of signature and revocation, and (ii) limited validity/revocation periods for keys. He then discussed the handshake protocol and various concepts of forward security.

Later Dr. Herzberg focused on obtaining security by redundancy. That is, the idea of sharing a secret among multiple redundant servers. He concentrated on issues such as the secure storage and retrieval of keys, and the minimum number of servers needed for recovery.

In the second half of the lecture, Dr. Herzberg discussed various topics such as polynomial secret sharing using Lagrange interpolation, verifiable secret sharing, asymmetric secret sharing (in which not all users are equally trusted). Finally, he spoke about the situation when all servers may be

corrupted and how one recovers from such a situation. He also spoke about proactive password security and proactive secret sharing and its applications. He concluded the talk reinstating the fact that key exposure is a major threat and current operating systems are insecure, and briefly indicating potential solutions to those problems.

2.8 Distributed Denial of Service Attacks and Software Security

Speaker: Angelos Keromytis

Dr. Keromytis began his talk by addressing various issues related to Internet attacks, such as spoofing, building-security at end points, etc. He pointed out that a partial answer to these problems is firewalls. Firewalls divide the world into trusted and untrusted entities. They also allow only authorized traffic to pass. He then described how firewalls operate at various levels of the TCP/IP stack. He discussed various problems concerning firewalls, and also discussed distributed firewalls.

Dr. Keromytis then addressed three major issues:

- Network denial of services (DoS)
- Remote software exploits
- Worms

He expanded on each of these issues. A DoS attack is easier to launch than other kinds of attacks. This can happen at the levels of CPU, memory, and OS tables. There are various types of DoS over a network. The person who launches a network DoS does not have to be a legitimate user and firewalls become a target for DoS attacks. The different types of DoS are (i) link congestion, (ii) router processing capacity, (iii) end-host (server) processing capacity. Reserving bandwidth, authentication and load balancing may offer some protection, but does not help with congestion attacks.

Later, Dr. Keromytis focused on distributed DoS (DDoS)—it is a coordinated attack on a target from many sources. He also discussed defenses against such DDoS attacks. Data replication techniques used by Akamai only work with static content. Attack prevention offers better security. The pushback mechanism can determine predicates and passes them to upstream routers to prevent attacks. There are also algebraic approaches to attack detection.

In the second half of the talk, he spoke about remote software exploits where the major vulnerabilities are the result of bad code, which cause buffer overflows, race conditions, and insufficient/incorrect argument validation. Finally, Dr. Keromytis spoke about worms, which are self-propagating malicious code. Their propagation speed exceeds human reaction. He discussed various protection mechanisms such as sandboxing, content filtering, and anti-worms.

2.9 Internet Crypto Tools

Speaker: Amir Herzberg

In this talk, Dr. Herzberg focused on transport layer security. SSL (the secure sockets layer) and TLS (transport layer security, the IETF standardized version of SSL) were the main focus of this talk. Both help to provide a secure TCP tunnel from client to server. He gave a brief description of how they evolved over the years. Both are easy to implement and are deployed in most web browsers and servers. Since TCP connections are not encrypted by default, the application layer must explicitly choose to use encryption. Another issue is that the TCP header is not encrypted.

He then proceeded to speak about adding security to the network layer. This provides security to all applications without additional effort. Since routers, operating systems, etc., are all aware of the encryption, not even header information is revealed. The downside is the difficulty of implementation. Next, he spoke about the various operational phases of SSL, and its services. In the SSL handshake protocol, the client and the server agree on the encryption algorithm and options. He spoke about the various session resumption issues, and also explained the various factors involved in designing applications using the SSL API. He also stated that validating certificates has to be done by the application and not by SSL itself. He finished this section of the talk by talking about the cryptographic issues in SSL and TLS.

In the second half of the talk, Dr. Herzberg focused on the second alternative for encrypted communication, namely IPsec, the secure alternative to the network layer Internet Protocol (IP). The network layer in the TCP/IP network protocol suite is characterized by connectionless, unreliable communication in which packet headers are easily spoofed, and gateways and routers are open to packet inspection. He listed the requirements for any secure network layer. IPsec is the IP security protocol for both IPv4 and IPv6. He listed all the services provided by IPsec. He explained that IPsec is

actually comprised of two layers, one for the negotiation of a secure connection, and the other to encapsulate and protect data. He listed alternatives to where exactly security is added, how exactly IPsec is implemented and the various modes of operation. In his concluding remarks he emphasized that IPsec protects all traffic, that it has flexible security policies for security, and that it is resilient to clogging.

2.10 Electronic Commerse: Payment Protocols and Fair Exchange

Speaker: Markus Jakobsson

In this talk Dr. Jakobsson spoke about some signature-based payment schemes, fair exchange, and micro-payment schemes. He began with credit card transactions and the pitfalls therein. He then spoke about the typical e-money in which all those pitfalls are avoided. This led to blind signatures, including the blind RSA signature scheme. In any scheme two basic user attacks need to be avoided— namely, forgery and overspending. Also, bank attacks needed to be prevented such as tracing, incrimination, embezzlement, and abuse of privacy. He said that what is needed is the ability to revoke privacy. The next part of the talk was about fair exchange. He spoke next about micro-payments and the need for small payments. Most digital cash schemes are unsuitable for micro-payments because of their high overhead. The way to handle micro-payments is by aggregating then into fewer macro-payments. Finally, he spoke about various possible micro-payment schemes.

2.11 Problem Sessions

Leader: Nelly Fazio

In addition to the lectures, each day included a one-hour "problem session" During these sessions, Ms. Fazio interactively led the tutorial participants in working through a number of exercises, some of which had been handed out the day before. These sessions were designed to make the learning experience more complete by giving participants a chance to try to solve some problems on their own and then see how well they had done.

3 Acknowledgements

The author of this report wishes to thank Dr. Rebecca Wright, and Dr. Brenda Latka for their valuable comments. Also, she thanks the primary and additional lecturers for their informative talks. The author and the DIMACS Center acknowldge the support of the National Science Foundation under grant number CCR 03-14161 to Rutgers University.