CPE5021
Advanced Network Security

--- Modern Computing and Network Security and Cryptography ---

Lecture 1

Schedule

- 1. Modern Computing and Network Security
- 2. Elliptic Curve public key system
- 3. Design and Implementation of RSA and ECC
- 4. Design, implementation and configuration of firewalls
- 5. Strengthening and managing firewalls and other network components
- 6. Intrusion Detection Systems: concepts and designs
- 7. Intrusion Detection Systems: implementation and configuration using Snort
- 8. Wireless security: principles and practice in depth
- 9. Security in trusted-based computing environments
- 10. Security, load balancing and network performance
- 11. Secure network architecture: design and implementation
- 12. Readings and discussion about future of Network Security
- 13. Test and guest speakers

Modern Computing and Network Security

- 1. Will the future networks be wireless and companies need to provide more wireless communications and services.
- 2. How can companies provide secure wireless communications for mobile users including users using mobile phones, or smart cards?
- 3. What can happen if computers double their computational capacity in every six months?
- 4. What will be the important factors in network security? Cryptography? Firewalls? VPN?
- 5. How can we provide adequate security for peer-to-peer communications?

Modern Computing and Network Security

- 6. Private key systems are still useful however, key distribution is a problem. Is there any way that this problem can be resolved without replying on public key technology.
- 7. Trusted-based computing environments will increase the efficiency of networks and Internet services, however security is a big concern. Which technology should be employed to provide adequate security for such environments.

Answers

- 1. The future networks will be wireless and companies need to provide more wireless communications and services.
  - The number of wireless customers and wireless networks in UK and USA has been increased quickly.
  - Several hardware and software vendors such as CISCO, IBM, Microsoft have focussed more on their wireless products, such as wireless routers (CISCO), Pervasive computing, Wireless Network Auditor, WebSphere (IBM), Wireless-G (Microsoft), etc.

Answers

- 2. How can companies provide secure wireless communications for mobile users including users using mobile phones, or smart cards?
  - Research on new cryptographic technology particularly Elliptic Curve Cryptography promises more efficient and secure solutions than that we currently have.

Answers

- 3. What can happen if computers double their computational capacity in every six months? (Quantum computing and optical computing) Especially fast computers with affordable price.
  - There will be millions of people who can have a chance to try to break the current cryptographic algorithms.
  - Super computers will be much faster and there is a high chance that many applications based on the existing cryptography will become vulnerable.
  - Hackers will have better machines to run their software to quickly find vulnerabilities in many systems which are not upgraded in time.
  - Many network components will need to be updated because of the update in cryptography, and the discovery of vulnerabilities due to the advance of technology.

Answers

- 4. What will be the important factors in network security? Cryptography? Firewalls? VPN?
  - Cryptography will be more important because of the demand for wireless communications, peer-to-peer communications, more Internet services, etc.
  - Firewalls will still play a critical role because many companies will still rely on firewalls to protect their networks. However, wireless firewalls need to be developed.
  - VPN role depends on the popularity of wireless communications.
  - IDS and Prevention Systems will play a critical role in future networks, especially national and international networks and trusted-based computing environments.

Answers

- 5. How can we provide adequate security for peer-to-peer communications?
  - New authentication techniques must be developed.
  - New cryptography must be developed for peer-to-peer wireless communications.
  - Digital signature technology should be improved to assist peer-to-peer communications.

Answers

- 6. Private key systems are still useful however, key distribution is a problem. Is there any way that this problem can be resolved without replying on public key technology.
  - Quantum cryptography will possibly be the solution.
  - Advanced cryptographic techniques can provide ways for secret key exchange without relying on a single permanent secret key.

Answers

- 7. Trusted-based computing environments will increase the efficiency of networks and Internet services, however security is a big concern. Which technology should be employed to provide adequate security for such environments.
  - The application of new digital signature technologies together with IDS will need to be developed.
  - New secure network architectures will need to be developed.

How to do it

- Searching for new cryptographic algorithms
  - Small key size.
  - Fast encrypting and decrypting and digital signature generation.
  - Require less computational power, more suitable for mobile devices such as mobile phones and smart cards.
  - Algorithms must be flexible and highly scalable.

How to do it

- Design and implement more efficient cryptographic algorithms for wireless communications. Eg. More research work on ECC and other cryptographic technology.
- Further research in pervasive computing (see Le et al's paper on " Mobile ticket engine").
- Design and implement better algorithms for peer-to-peer communications. E.g Design better authentication techniques that can provide more secure and better authentication (see Le's paper on "strong authentication for peer-to-peer communication", and Keng, Le, and Srini's paper on "Secure Internet payment system").
- Design and implement better firewalls for wired and wireless networks. E.g, (see SAFE firewalls from CISCO).
- Design and implement better IDS and Prevention Systems which allow different networks to work and support each other. E.g (proposed work from Le on trusted-based computing and cooperating networks).
- Design and implement better algorithms to balance security, load balancing, and network performance. (See Le's load balancing in distributed environments.)

(Please note that there are many other papers related to the above topics)

What will we do in CPE5021

- Theoretically discuss ECC and compare ECC and RSA. Then practically you will design and implement both algorithms to completely understand the two most important public key systems.
- Theoretically discuss all types of firewalls including wireless firewalls. You will then experiment the practical implementation and configuration of important types of firewalls including packet filtering and application-based firewalls.

What will we do in CPE5021

- Theoretically discuss quantum cryptography and emerging techniques for secure key distribution.
- Theoretically discuss the design and implementation of IDS. You will then practically experiment the Snort system to understand how important IDS in network security in the future.

What will we do in CPE5021

- Theoretically discuss wireless security in depth, including principles and techniques for software applications, network architectures and security design. You will have the opportunity to design and set up simple and secure wireless networks (this depends on whether we have time and you have some required equipments or not!). We currently only have a few APs.
- Theoretically discuss the design and implementation of secure network architectures. This will help you understand the fast-growing wireless networks, peer-to-peer communications and trusted-based computing environments.
- Theoretically discuss the relation between load balancing, network performance and security.

What will we do in CPE5021

- Theoretically discuss trusted-based computing and the role of IDS and digital signature. This will provide you an understanding of future software and networks.
- In order to understand the existing networks and security problems, you are required to do self-study on the existing systems, look for vulnerabilities and find proper techniques to show that possible attacks may occur to some of the existing systems (this work is strictly carried on your own system ONLY).

Conclusion

- Due to the short period of time (12 weeks), we cannot do as much as we wish to do.
- Practical works will give you a deep understanding of important theory in network security.
- The main focuses of CPE5021 are advanced cryptography, firewalls, IDS, wireless security, secure network architectures, peer-to-peer, pervasive and trusted-based computing environments.
- Please note that some popular security technologies today can become obsolete in the next few years.