70-72,75-77,79-89)

- Myths about digital signatures discussed by Ed Felten (R 18 83,84)
- Maryland attempting to outlaw 'annoying' and 'embarrassing' e-mail (R 18 81)
- Nevada contemplating outlawing unsolicited junk e-mail (R 18 87)
- Vineyard.NET spammed by VC Communications, sending 66,000 messages (R 18 79)
- More risks relating to spamming and spam blockers (R 19 02,05,10,13); legal implications (R 19 10)
- Phone calls to Moldova result from porn scam (R 18 80,83,84,87)

Report: 4TH ACM Conference On Computer and Communications Security

Donald J. Reifer, President
Reifer Consultants, Inc.

Introduction

The 4th ACM Conference on Computer and Communications Security [1] was held on 1-4 April 1997 in Zurich, Switzerland. About 100 participants from around the world gathered to discuss advances being made primarily in the area of defensive information warfare. This was primarily a research-oriented event which attracted principal investigators working in the security field from about 14 nations. I attended the conference for the following four reasons:

- I wanted to update my knowledge of the area.
- I wanted to ascertain what progress has been made in the field.
- I wanted to determine whether there were any breakthrough technologies on the horizon.
- I wanted to understand the threats being guarded against and the defensive strategies that leaders in the field were recommending.

As I will relate later, significant progress has been in many defensive information warfare areas. I particularly was impressed by the advances that have been made in the area of cryptography, digital signatures and communications protocols. I was disappointed by the perceived lack of progress over the years in the important area of trusted systems and information security infrastructure development.

This was the first conference that I have attended on the subject in about a decade. I selected the event because I thought that it would allow me to view both present work in the field and look into the future.

The Conference

The Conference began with a day of tutorials. I attended a morning session on the theory and applications of cryptography and an afternoon session on information warfare. Both were basic and summarized the field. The cryptography lecture was very enlightening. It discussed the Internet threats and how public and private cryptography key schemes help counter them. The information warfare lectures focused on defensive techniques; mainly because nobody seems to want to talk about offensive ones. It told us about how the good guys guard against and recover from breakins and active attacks. Speakers were knowledgeable and entertaining.

Two other tutorials were held. One focused on internet security architectures and the other on practical internet security for system and network administrators. I reviewed copies of both and found them interesting, but fundamental. The remaining three days was devoted to paper and panel sessions. Dr. Ross Anderson of Cambridge University's Computing Lab gave the keynote entitled: "Cryptography and security policy – towards a discipline of security engineering." Dr. Anderson discussed why crypto systems had failed over the last few years in terms of active attacks. As part of his discussing the lessons learned, Dr. Anderson suggested:

- Almost all other security failures occurred due to blunders in application design.
- Security goals in these cases were uniformly poorly understood.
- Attacks follow predictable patterns: first procedural, then opportunistic exploitation of design errors, and finally use of the latest technology to exploit weaknesses (code cracking via supercomputers, harvesting keystrokes captured outside of the physical plant through sophisticated recording devices, etc.).

The most memorable quote made during the entire conference was made by Dr. Anderson when he said: "Anybody who says the problem can be solved by cryptography neither understands the problem nor cryptography."

Next, the paper and panel sessions began. Topics covered during two and one half day's worth of sessions included:

- Authentication techniques and access controls
- Electronic commerce, banking and commercial security
- Defensive information warfare approaches
- Fair exchange of information protocols
- Internet and Intranet security
- Network management and smart card applications
- New directions in cryptography and key management
- Operating system security and trusted systems
- Programming languages and system security
- Public key and digital signature schemes
- Security evaluation and auditing techniques
- Theoretical foundations of security

Of course, the panel sessions were where most of the interesting comments were made. These tended to be lively and focused. I particularly enjoyed the panel on programming languages as the basis of security. Participants primarily argued the merits of protection schemes in languages and their associated run-time libraries.

The most innovative paper that I heard suggested the use of private keys to trigger public keys along with digital signatures for a mobile communications adversary. This scheme makes it very difficult to crack the cipher because it diffuses the key in space and time. Another paper that held my interest and seemed somewhat practical dealt with use of decision trees to perform proactive password checks.

Assessment and Conclusions

I achieved all of the objectives I set for the conference. I had some fun, met some interesting people and got a few good ideas. I updated my knowledge and came to the following conclusions relative to the progress being made in the field:

- If someone wants to breakin, they can given sufficient time and resources
- A large number of defensive tools and techniques exist to ward off attacks
- Significant advances seem to have been made in the areas of digital signature technology, communications protocols, and public and private key cryptography
- Limited progress seems to have been made in the areas of trusted systems and operating system security.
- The most significant threat facing companies today is the Internet because you don't know whether its software (user programs, plugins, libraries, tools, etc.) is threat

With regard to breakthrough technologies, I didn't see any on the horizon. I did, however, gain some insight into the threats being guarded against which include, but are not limited to, the following examples:

- Black box attacks - Outsider collusion - Password harvesting
- White box attacks - Insider collusion - Backdoors, trojan horses, viruses, etc.
- End run attacks - Key compromises - Secret sharing
- Active attacks - Opportunistic exploitation of - Code cracking - system bugs - Wiretapping

For Those Interested in Security Conferences

The following conferences and workshops might be of interest to you if you want to investigate this topic this fall. These meetings tend to be very theoretical with few industry people being involved. Those that are tend to come from Labs or research organizations.

- 1997 Information Security Workshop (ISW '97), Ishikawa High Tech Conference Center, Japan, 17-19 September 1997.
- International Conference on Information and Communications Security, Beijing, P.R. China, 11-13 November 1997.
- Thirteenth Annual Computer Security Applications Conference, San Diego, California, 8-12 December 1997.

The 5th ACM Conference on Computer and Communications Security will be held in th fall of next year in San Francisco, California.

References

1. Association for Computing Machinery, **Proceedings of 4th ACM Conference on Computer and Communications Security**, April 1997.