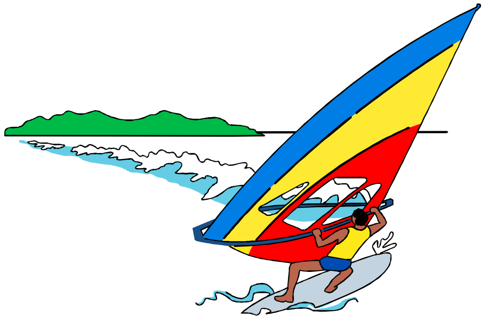
Perspectives on Progress and Directions for Network Security Research



Hilarie Orman

Network and Distributed System Security Symposium (NDSS ‘99)

Feb. 1999

Network Security: The First Plateau

- Only 25 years later …
- Commercial IPSEC
- Widespread SSL
- PGP in products
- Certificates no longer seem weird
- Secure key exchange standards
  - IEEE, ANSI, ATM, IETF
- Who could ask for anything more?

Government Concerns

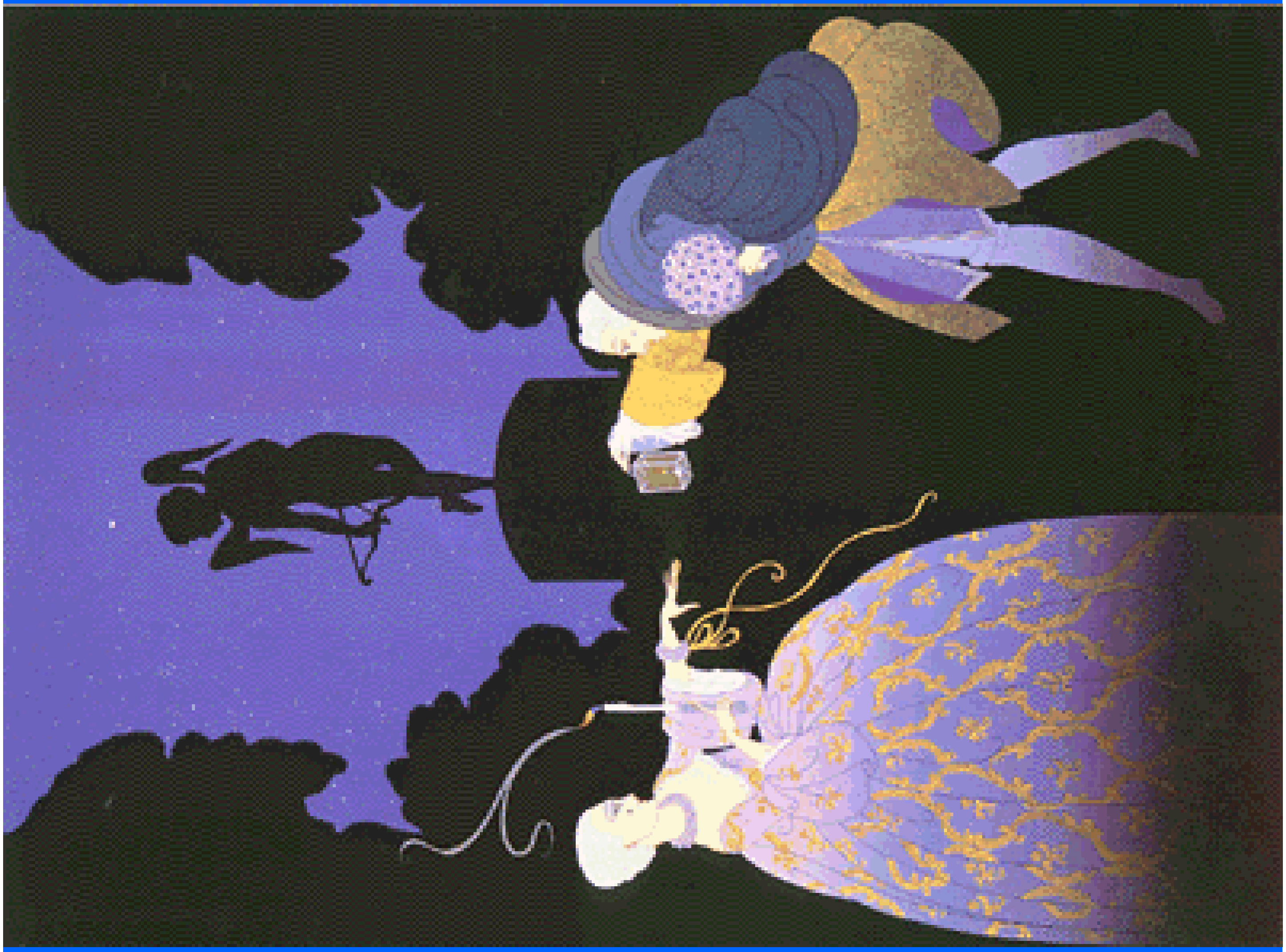
- Manageable security
  - Roles, cross-certification, CA’s
- Flexible policy
  - Federal, state, local governments
  - Coalition partners
- Risk assessment
- All eggs in the network basket?
  - Peacetime infrastructure
  - Wartime infrastructure
  - Coordinated attacks, coordinated defense

Industry Concerns

- End-to-end confidentiality clashes with network management
- Managing VPN configurations to match inter-organizational policy
  - the return of MLS?
  - Merge secure multicast with secure VPN?
- Performance impacts
- Preservation of intellectual property
- Security-correct software

New Network Security Concerns

- Embedded devices meet the Internet
  - The Internet washing machine’s repair history
  - Can a toaster take down the Internet?
- Sensor networks
  - Thousands of small sensing/actuating devices with wireless communication
  - Is their data reliable?
  - Is access safely authorized?
  - Can the network be turned against “us”?



The Next Plateau: Research Areas

- Secure group communication
  - Efficient sender authentication
  - Group management
  - Secure Multicast routing
  - Secure VPN vs. Secure Multicast
- Mapping policy to mechanism across organizations
  - Policy representation, negotiation, enforcement, consistency

Research Areas

- High-speed networks
  - Cryptography in the optical domain
- Practical mobile security
- Integrity of autonomous devices
- Strong availability guarantees
  - A scientific/engineering basis for risk assessment??
  - Strong redundancy guarantees and monitors
- Smart attack/corruption detection, adaptive and automated response

New Political Concerns

- Coordinated attack detection requires widespread monitoring and correlation
- Certificates tied tightly to liability
- The authenticity of and access to the on-line government
- Madness of crowds