Several Security Issues

Yvo Desmedt
Department of Computer Science
University of Texas at Dallas

September 16, 2016
1. Reliable and Private Communication

Classical results

This goes back to World War I, after the cable ship Telconia lifted from the bed of the North Sea the German overseas telegraph cables:
• **What is it?** Sender and a receiver do not share keys. They want to privately and reliably communicate over a network provided that the number of nodes (or edges) the adversary can control is limited and that the network has enough connectivity.

• **Potential applications:** Prevent Denial of Service, backup in case public key is broken, protect against a death-switch.

• **Results achieved on:**
  1. *Ethernet like networks:* solved a 13 year open problem (by Franklin-Wright)
  2. *Point-to-point networks:* generalized Kurosawa-Suzuki’s Eurocrypt 2008 result
  3. *Almost Secure Message Transmission* (slightly relaxed security): more efficient protocols
4. The directed graph case: introduced the problem, found conditions for special case.

5. Other results: showing others wrong, color adversary structures.

- Illustrative examples:
The importance of color based access structures has become clear in the following contexts:

- Cisco Faces Challenges As Chinese Media Urge Switching To Domestic Products For National Security Reasons In Wake Of NSA Surveillance Leaks
  

- BT’s use of Huawei’s equipment:
UK security committee ‘shocked’ over Huawei contract with BT

By James Blitz and Daniel Thomas

A parliamentary committee has attacked the British
2. Secret Sharing and Threshold cryptography

- What is it? Secret sharing allows backup of data in a reliable and private manner.

- Potential applications:
  1. Cloud storage (post Snowden)
  2. Distributed security: the foundation of many tools, such as Reliable and Private Communication (see also later)

- Results achieved on:
  1. threshold cryptography: foundations, several new schemes
  2. Secret sharing: linking bounds to combinatorics (orthogonal array)
  3. Redistribution of shares: introduced in the most general case, making it verifiable
  4. Functional secret sharing: introduced the concept, first schemes
3. Voting

- Plurality voting is not optimal:

<table>
<thead>
<tr>
<th>Most preferred candidate:</th>
<th>Voter 1</th>
<th>Voter 2</th>
<th>Voter 3</th>
<th>Voter 4</th>
<th>Voter 5</th>
<th>Voter 6</th>
<th>Voter 7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Second preferred candidate:</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Least preferred candidate:</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

- Results achieved on:
  1. Equilibria of plurality voting with abstentions, e.g., is sequential voting better?
  2. Hacking Helios 2.0, an Internet voting scheme using lots of cryptography
  3. Copying votes: secret endorsements
  4. Hacking resistant voting: unconditionally secure Internet voting scheme (using secret sharing)
  5. Other results: e.g., keeping the tally private
4. Secure multiparty computation

- **What is it?** Parties $P_1, P_2, \ldots, P_n$ knowing respectively $x_1, x_2, \ldots, x_n$ want to privately compute $f(x_1, x_2, \ldots, x_n)$, i.e., nothing leaks more than what follows from the output.

- **Potential applications:** Private cloud computing, privacy in general. Example: bank loan

- **Results achieved on:**
  1. Using black-box groups to perform secure multi-party computation
  2. Reduce the use of VSS to make it more practical
  3. Non-interactive dealer in VSS
  4. Asymmetric Trust and its applications in secure multi-party computation
Some details:

Sun-Yao-Tartary (2008) made a link with perturbation theory.
5. Critical infrastructures

- Results achieved on, e.g.:
  1. Robust Operations, i.e., how to make a robust variant of an operational research problem?
  2. Identifying critical infrastructures, e.g., using AND/OR graph models
  3. Analyzing concrete vulnerabilities, e.g., potential weaknesses of Internet Banking
  4. Anti-jamming networks and constructing resilient data networks
6. Viruses, malware and computer security

Results achieved on:

1. Hardware virus

2. Virus in LaTeX

3. Using LinkedIn for Spear phishing (unpublished)

4. Cryptographic Authentication to protect

5. Malware to demonstrate:
   • Vulnerability of two-factor authentication in Internet Banking
   • Vulnerability of Internet voting systems

6. Use of NOP to achieve Software Diversity

7. Function Based Access Control
7. Other

- Results achieved on:
  1. Privacy in social networks, e.g.,
     i. privacy in Facebook versus Google+
     ii. Cloak attack against Facebook (20,000 newspapers reported about it)
  2. Efficient and proven secure hybrid encryption
  3. Efficient key stream authentication using combinatorics
  4. Key distribution, e.g., for conferences using pairing based cryptography, or non-malleable while robust against active adversaries
  5. Cryptanalytic study, e.g., of E0, Luffa, Rabbit Shannon Cipher