The Challenge of Data and Application Security and Privacy (DASPY)

Ravi Sandhu
Executive Director and Endowed Professor
March 23, 2011

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Fundamental Premise

- Cyber security is all about trade-offs
  - confidentiality
  - integrity
  - availability
  - usage
  - privacy
  - cost
  - usability
  - productivity

- Application context is necessary for trade-offs
The ATM (Automatic Teller Machine) paradox

Lessons from the Orange Book era

Data security and privacy

Application security

The DASPY system challenge

DASPY research thrusts
The ATM system is secure enough and global in scope. However, it is not attainable via current cyber security science, engineering, doctrine. Similar paradoxes apply to on-line banking and e-commerce payments.
Monetary loss is easier to quantify and compensate than information loss.

- Security principles
  - stop loss mechanisms
  - audit trail (including physical video)
  - retail loss tolerance with recourse
  - wholesale loss avoidance

- Technical surprises
  - no asymmetric cryptography
  - no anonymity
Monetary loss is easier to quantify and compensate than information loss.

Security principles: Application Centric
- stop loss mechanisms
- audit trail (including physical video)
- retail loss tolerance with recourse
- wholesale loss avoidance

Technical surprises
- no asymmetric cryptography
- no anonymity
Our Basic Premise
- Security is fundamentally about tradeoffs
- There can be no security (no tradeoffs) without application context

Orange Book/Rainbow Series (1983-94)
- Security is all about high assurance
- Application context makes high assurance security impossible to achieve
34 titles listed in Wikipedia as the “most significant Rainbow series books”
- Only 1 addresses applications
- Trusted Database Interpretation (TDI)
- Scope: “Trusted Applications in general and database management system in particular”
The Polyinstantiation Wars

<table>
<thead>
<tr>
<th>Software Architect</th>
<th>Project</th>
<th>% Time</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>Win7</td>
<td>25%</td>
<td>U</td>
</tr>
<tr>
<td>Alice</td>
<td>SecureWin7</td>
<td>75%</td>
<td>S</td>
</tr>
<tr>
<td>Bob</td>
<td>Vista</td>
<td>100%</td>
<td>U</td>
</tr>
</tbody>
</table>

- **What precisely is Secret?**
  - There exists a SecureVista project
  - Alice works on SecureVista
  - Alice’s effort on SecureVista is 75%
  - All or some of the above

- **How do we maintain integrity of the database?**
  - Depends

---

Much work and $$$ by researchers and vendors, late 80’s-early 90’s
Familiar term used for over 3 decades

Fundamental problems identified in the first decade continue to dominate
- covert channels
- inference and aggregation
- homomorphic encryption

“The general understanding of the term data security and privacy is probably not significantly changed since these early days, although of course in the details and nuances there have been considerable advances.” -- Sandhu, CODASPY11
Has come into use relatively recently
  - Remains amorphous

The How interpretation: (currently prevalent in industry)
  - scanning for software vulnerabilities such as buffer overflow
  - run time application firewalls to prevent/detect application layer attacks

The What interpretation: (the bigger challenge)
  - security policy and trade-offs in existing applications such as on-line banking: relatively straightforward and relatively well understood
  - security policy and trade-offs in newer applications such as social networks, secure information sharing, smart grid, secure data provenance, location-based services, electronic health records: much fuzzier, less familiar and a major challenge to understand
Wisdom from the past:

“Generally, security is a **system problem**. That is, it is rare to find that a single security mechanism or procedure is used in isolation. Instead, several different elements working together usually compose a security system to protect something.” R. Gaines and N. Shapiro 1978.

The DASPY system challenge is how to develop a systems perspective on DASPY.
The DASPY System Challenge

Security and system goals (objectives/policy)

- Necessarily informal

Policy models

- Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.
- Security analysis (objectives, properties, etc.).

Enforcement models

- Approximated policy realized using system architecture with trusted servers, protocols, etc.
- Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).

Implementation models

- Technologies such as Cloud Computing, Trusted Computing, etc.
- Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

Concrete System

- Software and Hardware

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Operational aspects

- Group operation semantics
  - Add, Join, Leave, Remove, etc
  - Multicast group is one example
- Object model
  - Read-only
  - Read-Write (no versioning vs versioning)
- User-subject model
  - Read-only Vs read-write
- Policy specification

Administrative aspects

- Authorization to create group, user join/leave, object add/remove, etc.
Group-Centric Sharing Enforcement Models

User Attributes: {id, Join-TS, Leave-TS, ORL, gKey}
Object Attributes: {id, Add-TS}

User Attributes: {id, Join-TS, Leave-TS, ORL, gKey}
Object Attributes: {id, Add-TS}

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Continue to pursue
- point solutions for various problems in data security and privacy
- solutions on the how aspect of application security

Embark on research to understand the what elements of application security
- There are some excellent examples already but this thrust needs further and explicit encouragement.

Embark on research to address the DASPY system challenge
- Today this is largely ignored.
First ACM Conference on Data and Application
Security and Privacy

ACM CODASPY 2011

Feb 21-23, 2011 | Hilton Palacio Del Rio | San Antonio, TX, USA.

The deadline for early registration is January 27, 2011.

Announcement

ACM SIGSAC announces the creation of a new annual ACM Conference on Data and Applications Security and Privacy. The inaugural conference will be held February 21-23 2011 in Hilton Palacio Del Rio, San Antonio, Texas.

About

With rapid global penetration of the Internet and smart phones and the resulting productivity and social gains, the world is becoming increasingly dependent on its cyber infrastructure. Citizens, firms, and producers of all kinds have learned to exploit this landscape much quicker than defenders have advanced in their technologies. Security and Privacy has become an essential concern of applications and systems throughout their lifecycle. Security concerns have rapidly moved up the software stack as the Internet and web have matured. The security, privacy, functionality, cost and usability tradeoffs necessary in any practical system can only be effectively achieved at the data or application layers. This new conference provides a dedicated venue for high-quality research in this area, and seeks to foster a community with the focus in cyber security.

Best Paper Award Committee

Goi Joon Ahn (Arizona State University)
Elena Femia (University of Insubria)
Dan Thomson (Sandia National Labs)

Maintained by:
Institute for Cyber Security
UTSA