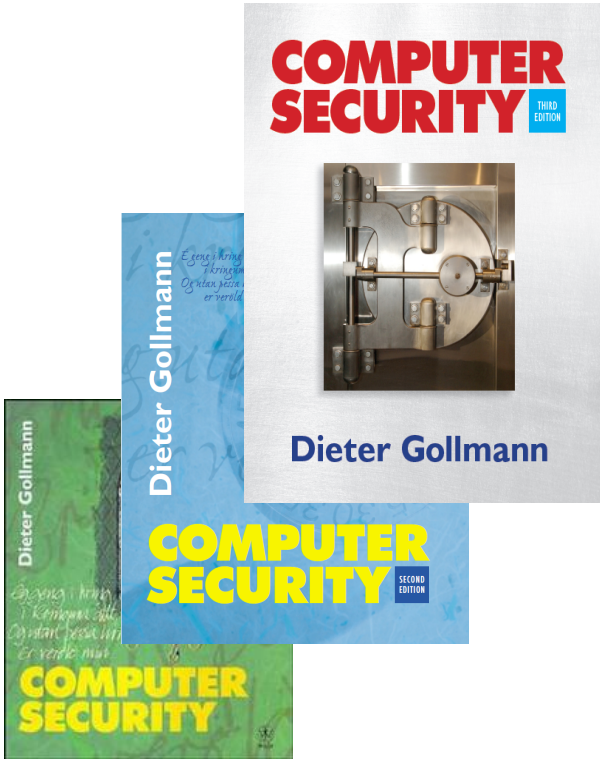
Closing Note

Dieter Gollmann
Hamburg University of Technology

TUHH
Technische Universität Hamburg-Harburg

Where I am coming from …

Ég geng i hring
i kringum allt, sem er.
Og utan Þessa hrings
er veröld mín.



NordSec 2013

- The 18th Nordic Conference on Secure IT Systems will take place at the Arctic Hotel in Ilulissat, Greenland, from 18th to 21st October 2013.

- http://nordsec2013.imm.dtu.dk/

Starting point – Computer security

The problem arises from a combination of factors that includes: the extension of resource sharing concepts to networks of computers; and the slowly growing recognition of security inadequacies of currently available computer systems.

[Anderson Report, 1972]

Thesis 1

- The problem is not “the emergence of complex resource sharing computer systems” but the inability to talk about such systems.

- We must use language fit for discussing the phenomena we want to investigate.

The meaning of words

When **I** use a word, it means just what I choose it to mean — neither more nor less.

~~Humpty Dumpty~~

Wittgenstein

CERT Advisory CA-2000-02

- Malicious HTML Tags Embedded in Client Web Requests
  - What makes a tag malicious?
- Because one source is injecting code into pages sent by another source, this vulnerability has also been described as “cross-site” scripting.
  - Can we have XSS without scripts??

Understanding an attack

- Via the method by which it is executed?
  - E.g. code injection
- Via the violation of a security property within the system?
  - E.g. elevation of privilege
- Via the violation of a security property of the application?
  - E.g. cookie stealing in violation of SOP

Thesis 2

XSS is an access control problem.

Access Control

- There exists a language (conceptual framework) for discussing access control since the 1980s (at the latest).

- There are principals, subjects, objects, access operations (access rights), and reference monitors.

Subjects and principals

- A principal is an entity that can be granted access to objects or can make statements affecting access control decisions [aka delegation].
- Subjects operate on behalf of principals; access is based on the principal's name bound to the subject in some unforgeable manner at authentication time.

  [M. Gasser et al.: The Digital Distributed System Security Architecture, NCSC 1989]

- "Subjects speak for principals."

Once upon a time …

- Principal names [had to] be globally unique, human-readable and memorable, easily and reliably associated with known people.
- So called identity-based access control or – better – user-centric access control.
- Life was simple: policy owner = policy enforcer = resource owner

… but times are changing

- Applications are becoming the new principals!
- Principals need to have names so that policies can refer to them.
  - How to name an application? Unique names?
- Access requests need to be authenticated.
  - Which principal is a subject speaking for? CSP!
- Principals need to be authorized.
  - CORS?

Mad New World

- Whose interests are captured by the policy?
- Why does the browser “trust” the policy received?
- Why does the server “trust” that the policy is enforced?

Security model for applications

- If applications are the new principals, what are the new subjects?
  - Units of computation bound to a principal in some unforgeable manner at authentication (?) time.

- The title of W3C Draft Runtime and Security Model for Web Applications is promising.
  - The security model will have to go beyond an interface standard to meet its promise.

Closing Note

- Roger Needham:
  Internet times; the wheel of reincarnation is spinning faster.

- Let's spin the wheel.


qujanaq