RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Security Principles versus the Real World

SESSION ID: CISO-T07

Moderator: Gary McGraw, Ph.D.
Chief Technology Officer, Cigital
@cigitalgem

Panelists: Eugene (spaf) Spafford
Director of Cerias
Purdue University

Marcus Ranum
CSO
Tenable

Jim Routh
CISO
Aetna

Keith Gordon
Vice President
Information Security & Risk Management

Introducing the Panel

Representing “The Principles”

- spaf, Purdue
- Marcus Ranum, Tenable

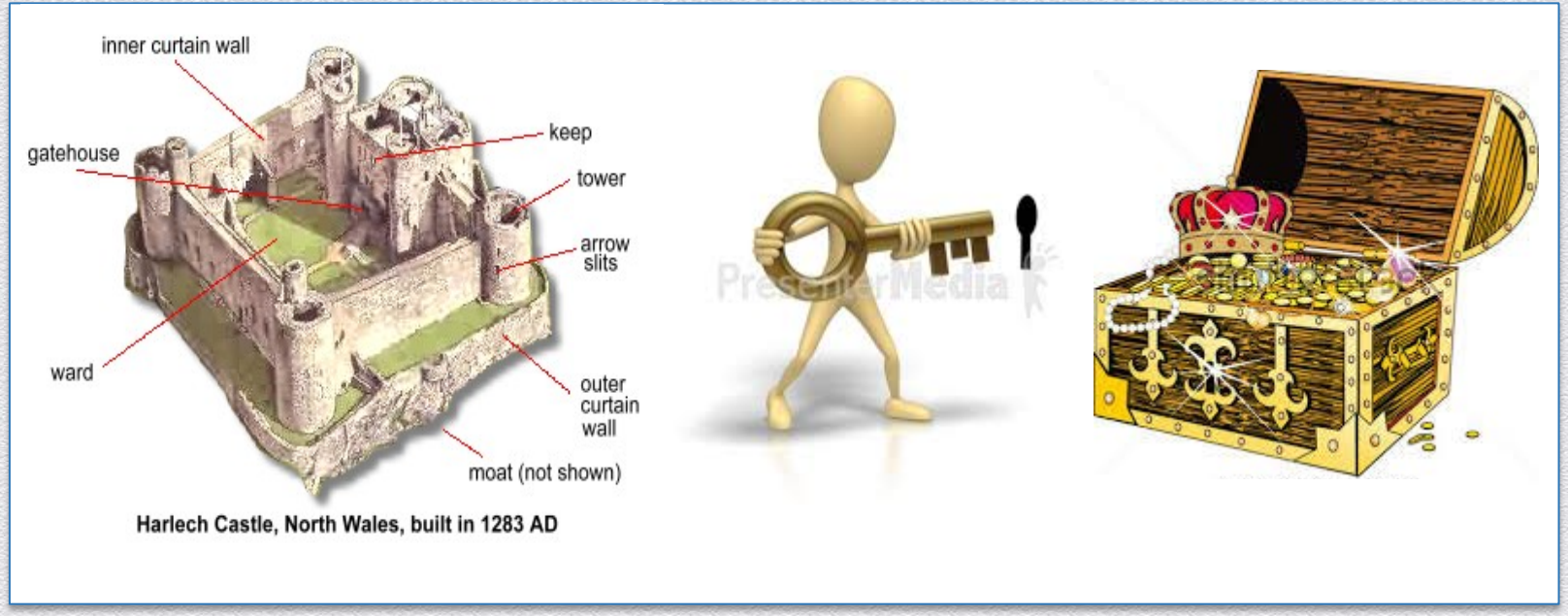
Representing “The Real World”

- Jim Routh, Aetna
- Keith Gordon, Capital One

Introducing the Principles

- Least privilege
- Least common mechanism
- Open design
- Economy of mechanism
- Fail-safe defaults

- Originally identified by Saltzer and Schroeder, these five principles are essential to security engineering



Least Privilege, or Keys to the Kingdom?

For centuries, unwarranted access has defeated the most sophisticated defenses, and compromised the most sensitive assets!

Least Common Mechanism

Minimize the amount of mechanism common to more than one user and depended on by all users.

From www.millenialmainframer.com

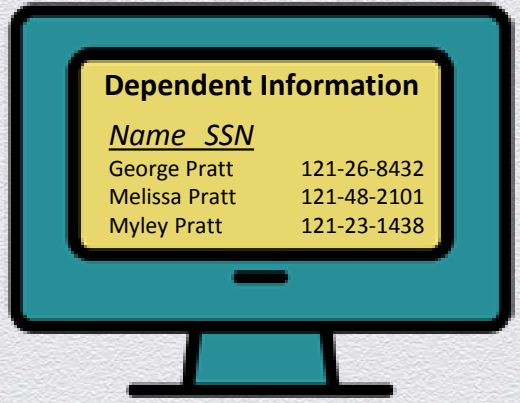
What one man can invent another can discover.

– Sherlock Holmes, The Adventure of the Dancing Men

OFFICER: We've analyzed their attack, sir, and there is a danger. Should I have your ship standing by?
TARKIN: Evacuate? In our moment of triumph? I think you overestimate their chances!

Open Design

The security of physical products, machines and systems should not depend on secrecy of the design and implementation.

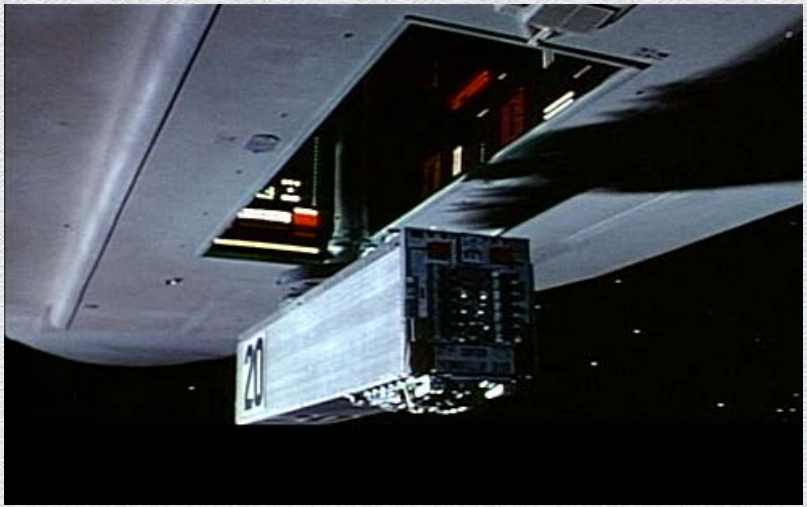


Example: Health insurance enrollment systems that require input of sensitive personal information that already exists in the system.

Economy of Mechanism

Keep the design as simple and small as possible.

Your bomb should be designed to prefer *not* to blow up.



Reformat hard drive? Press ‘N’ to abort, or any other key to continue

Fail Safe Defaults

A mechanism that, in the event of failure, responds in a way that will cause no harm, or at least a minimum of harm, to other devices or danger to personnel.

Open discussion

Compromise is often necessary. How closely do we adhere to the principles versus being flexible?

What do we measure to shed light on our posture WRT the principles?

How do we manage a real security program with restrictions and limitations without compromising the principles?