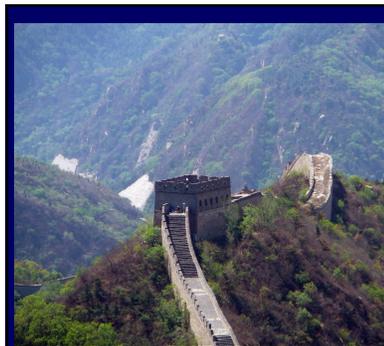


## What Every Computer Scientist Should Know About Security



David Evans  
University of Virginia  
<http://www.cs.virginia.edu/evans/>

cs290 Spring 2008  
21 February 2008

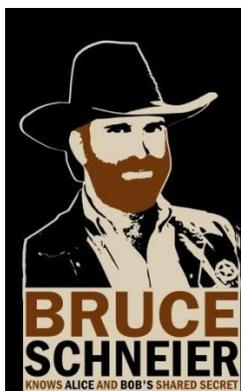
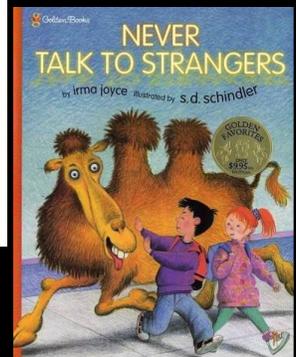
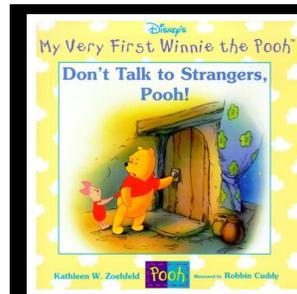


## What Every Human Should Know About Security

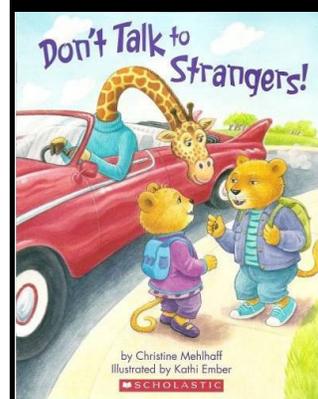
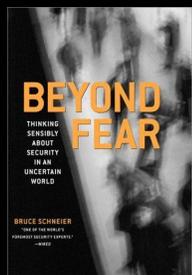
David Evans  
University of Virginia

cs290 Spring 2008  
21 February 2008

[www.cs.virginia.edu/evans/](http://www.cs.virginia.edu/evans/)



“Many children are taught never to talk to strangers, an extreme precaution with minimal security benefit.”



“Emma Lion loves to make new friends, but Mama tells her to be careful and never talk to strangers. Emma sees new people to meet everywhere she goes. How will she know who is a stranger?”



## Security Research

study of systems in the presence of *adversaries*

about what happens when people **don't** follow the rules

7

## Security

- Technical questions
  - Figuring out who is not a “stranger” (*authentication*)
  - Controlling access to resources (*protection and authorization*)
- Value judgments
  - Managing risk vs. benefit (*policy*)
- Deterrents
  - If you get caught, bad things happen to you

**Protecting assets from misuse**

8

## Quiz

Authentication, Protection, Authorization, Policy, or Deterrent?

9



Authentication, Protection, Authorization, Policy, or Deterrent?

10

Authentication, Protection, Authorization, Policy, or Deterrent?



Charlottesville Airport, Dec 2001

Authentication, Protection, Authorization, Policy, or Deterrent?

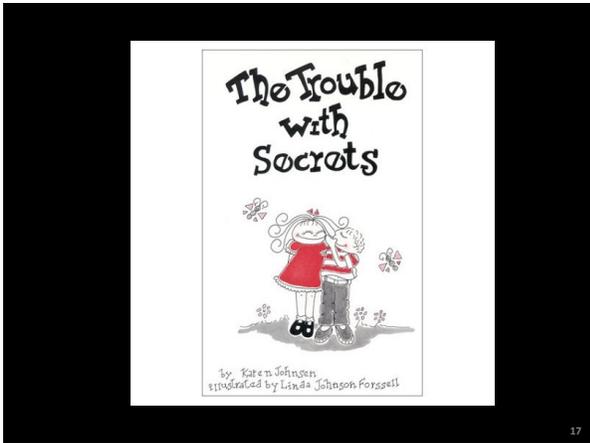


British Parliament, Dec 2007

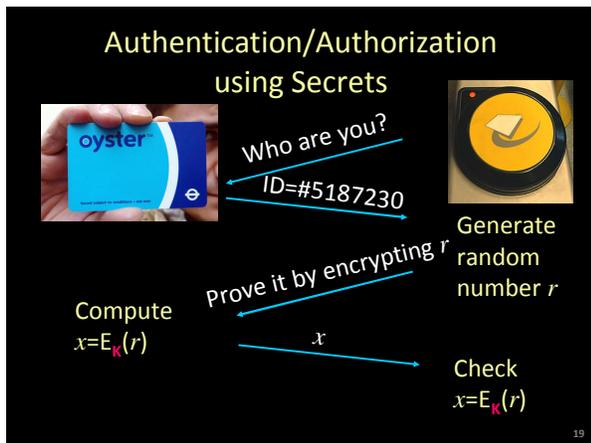
# Principles for Designing and Building Secure Systems

**Principle 0:**  
 Know what you are protecting, and what the threats are.

**Principle 1:**  
 Keeping secrets is hard.  
 Design systems so that they don't depend on secrets being kept from adversaries.  
 If you need a secret, make it small and well defined.  
 Kerckhoffs' principle, 1883



## Authorization with "Secrets"



### Encryption

- $E$  is an encryption function: algorithm for scrambling bits in a way that depends on  $K$
- $K$  is a secret key shared between card and reader (backend database)

$$x = E_k(r)$$

**Threat:** Eavesdropper cloning cards.  
**Requirement:** attacker who overhears  $x$  and  $r$  (even many pairs) should not be able to guess  $K$

20

### Recall Principle 1:

Keeping secrets is hard.

Design systems so that they don't depend on secrets being kept from adversaries.

If you need a secret, make it small and well defined.

Security should depend only on keeping  $K$  secret (not on keeping algorithm or protocol secret)

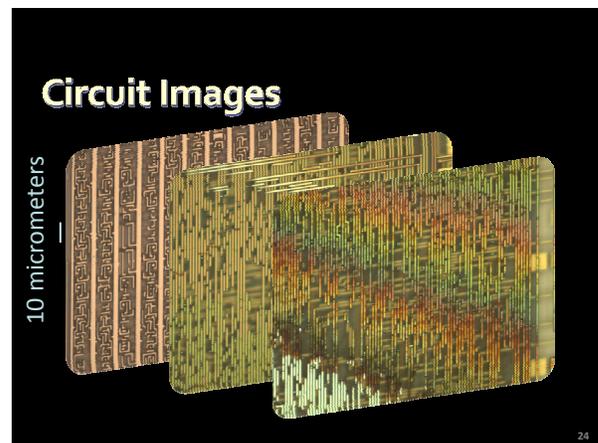
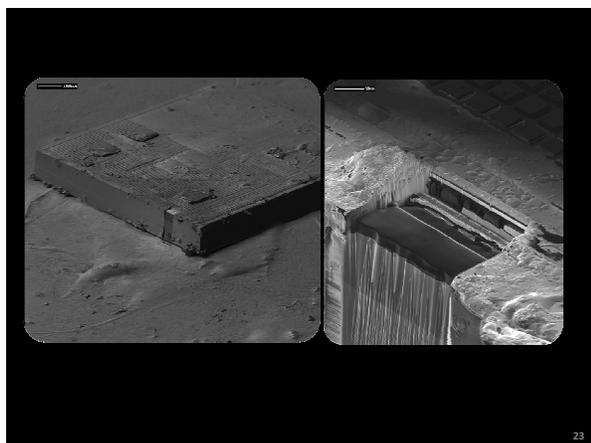
21

### NXP Mifare Classic RFID Tag

- Billions of units deployed
- Cost < \$1
- Planned for nationwide deployment in Netherlands
- Uses secret encryption algorithm

*Reverse-Engineering a Cryptographic RFID Tag.*  
 Karsten Nohl, David Evans, Starbug, Henryk Plötz, Feb 2008.

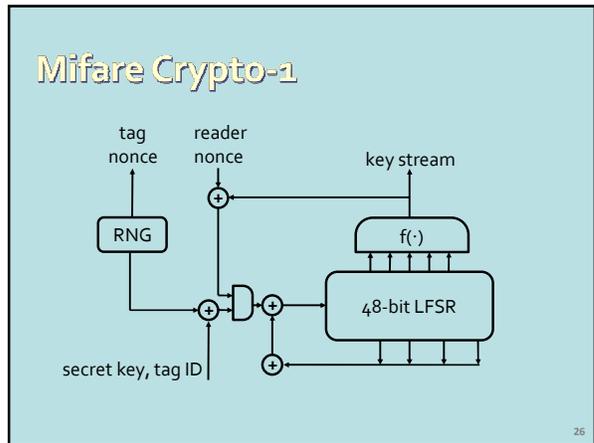
22



### Reverse Engineer Circuit

Very error-prone and tedious process (but can be automated)

25



### Does knowing E matter?

Who are you?  
ID=#5187230

Generate random number  $r$

Prove it by encrypting  $r$

Compute  $x = E_K(r)$

Check  $x = E_K(r)$

27

### Failure of Security through Obscurity

- If there are enough possible keys, it shouldn't matter if attacker knows E (if it is a good encryption algorithm)
- Mifare algorithm has several weaknesses that made it easier to find  $K$  without needing to try all possible keys

28

"The debate about the OV-Chipcard is symbolic, as we discovered yesterday at the hearing, for the choice: open or closed software. The bankruptcy of closed source software shone solidly in the limelight yesterday. GroenLinks [a Dutch political party] has urged for a long time that the government should work with open-source software. Yesterday it became painfully obvious that we may pay a high price due to the fact that this advice was not followed for the OV-Chipcard."  
 – Dutch parliamentary discussion, January 16th 2008

29

### Principle 2: Need to Know Basis

Once you release information, there is no way to get it back.

Give out as little as necessary to enable useful things.

Principle of "Least Authority"

30

## Facebook Platform

Generated by "untrusted" third party

Generated by Facebook

*Privacy-by-Proxy. Adrienne Felt, David Evans, Feb 2008.*

31

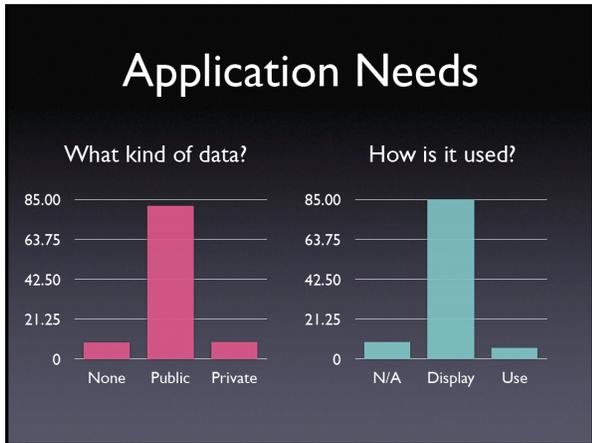
### Add TV Shows to your Facebook account?

Allow this application to...

Know who I am and access my information

Granting access to information is required to add applications. If you are not willing to grant access to your information, do not add this application.

32

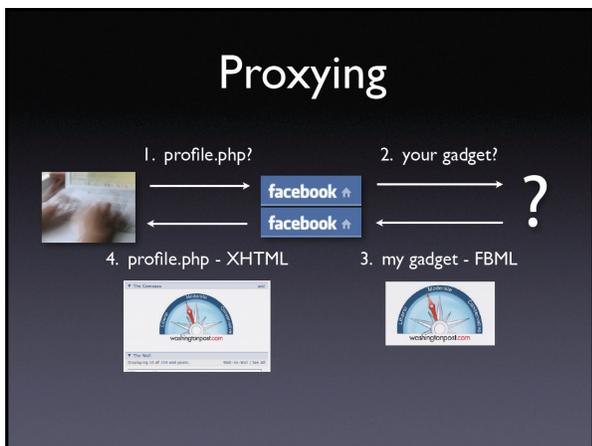


## Recall Principle 2: Need to Know Basis

Once you release information, there is no way to get it back. Be careful about what you release.

**No need to give applications access to information they don't use**

34



### UVA Today

#### U.Va. Engineering School Student Probes Facebook's Vulnerabilities

January 30, 2007 — Facebook, the social networking platform that has redefined communications, has millions of users. According to University of Virginia computer science major Adrienne Felt, all of these users should be concerned about security.

Felt, a fourth-year student in the School of Engineering and Applied Science at U.Va., leads a research project on privacy issues surrounding social networking platforms and is investigating the information sharing that occurs when users download a Facebook application — a program that allows the user to interact with other users in interesting ways, from sharing music to playing games.

Although these applications add variety to a Facebook user's profile page, they also increase the user's vulnerability. Here's how: anyone with an account on Facebook can create an application. Although this application appears as if it's part of Facebook's platform, it is actually running on application developer's server. When a user installs an application, that application's developer is given the ability to see everything the user can see — name, address, friends' profiles, photos, etc.

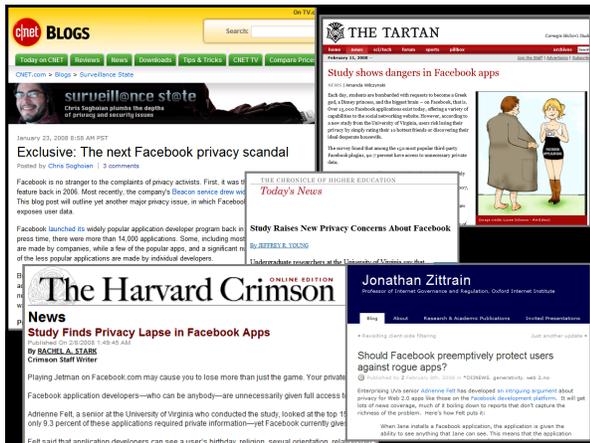
"The Facebook privacy policy always seemed unsatisfactory to me," said Felt, an experienced Facebook application developer.

It was this unsettling feeling that led her to investigate Facebook's vulnerabilities as a student researcher working with David Evans, an associate professor in U.Va.'s Department of Computer Science. With the help of fourth-year physics major Andrew Srinivas, Felt examined the 150 most popular Facebook applications. She discovered that 8.7 percent of these applications needed no personal information to run, while 52 percent needed only the user's public information (name, network, list of friends). Still, 93.3 percent require a user's private information in order to function.

"Since all applications receive access to private information," said Felt, "this means that 93.3 percent of Facebook's most popular applications unnecessarily have access to private data."

There are currently no restrictions on what applications (and their developers) can do with user data, and though the Facebook "Terms of Use" warn developers not to abuse the data they have access to, Facebook cannot enforce this rule, Felt says. In fact, when a user installs an application, the user's computer communicates with the

36



## from c|net article:

I asked Facebook's [chief privacy officer] Kelly what his company is doing to ensure that application developers do not violate the rules by saving a copy of user data that passes through their servers. He cited "extensive security mechanisms operating behind the scenes," although, he refused to expand on this, due to "security reasons." He wasn't too happy when I accused him of practicing **security through obscurity**, a concept widely mocked in security circles. He dismissed my charge as a mischaracterization.

## Recap

- Principle 0: Know what you are protecting, and what the threats are.
- Principle 1 (security-through-obscurity doesn't work): Design systems so that they don't depend on secrets being kept from adversaries.
- Principle 2 (least authority): Give others what they need to do useful work, but not more.

Not everything you need to know about security

## Questions

<http://www.cs.virginia.edu/evans>

My home page

<http://www.cs.virginia.edu/wheel>

Research group blog

If you steal property, you must report its fair market value in your income in the year you steal it unless in the same year, you return it to its rightful owner.

[\*Your Federal Income Tax, IRS Publication 17 \(p. 90\)\*](#)